CLAIMS

What is claimed is:

Sub a1

1. A computerized method for fast virus scanning of a file comprising:

storing anti-virus state information for the file in a data structure associated with the file and managed by a file system; and

obtaining the anti-virus state information for the file from the data structure when the data structure has been retrieved by the file system.

2. The computerized method of claim 1, wherein the data structure is a directory entry for the file and the anti-virus state information is stored in a field in the directory entry.

3. The computerized method of claim 2, further comprising:

partitioning the anti-virus state information into segments, each segment being equal in size to one of a plurality of fields in the directory entry.

4. The computerized method of claim 2, further comprising:

creating at least one field in the directory entry.

5. The computerized method of claim 1, wherein the data structure is an extra file fork for the file.

6. The computerized method of claim 5, further comprising creating the extra file fork to hold the anti-virus state information.

7. The computerized method of claim 1, wherein the data structure is stored as a resource within a resource fork for the file.

8. The computerized method of claim 1, further comprising:

encrypting the anti-virus state information before storing it in the data structure; and

decrypting the anti-virus state information when it is obtained from the data structure.

9. The computerized method of claim 1, further comprising:

comparing the anti-virus state information stored in the data structure against corresponding information associated with a current version of the file to determine if virus scanning is required; and

updating the anti-virus state information if the file is scanned as a result of the comparison.

10. The computerized method of claim 1, wherein data structure is retrieved by the file system as a result of the file being accessed by an application program.

11. The computerized method of claim 1, wherein data structure is retrieved by the file system as a result of a user requesting the file be scanned.

12. The computerized method of claim 1, wherein data structure is retrieved by the file system as a result of the file being in a pre-defined list of files scheduled for scanning.

13. A computer-readable medium having stored thereon executable instructions that cause a computer to execute a virus scanning method on a file, the method comprising:

storing anti-virus state information for the file in a data structure associated with the file and managed by a file system; and

obtaining the anti-virus state information for the file from the data structure when the data structure has been retrieved by the file system.

14. The computer-readable medium of claim 13, further comprising:

encrypting the anti-virus state information before storing it in the data structure; and

decrypting the anti-virus state information when it is obtained from the data structure.

15. The computer-readable medium of claim 13, further comprising:

comparing the anti-virus state information stored in the data structure against corresponding information associated with a current version of the file to determine if virus scanning is required; and

updating the anti-virus state information if the file is scanned as a result of the comparison.

16. The computer-readable medium of claim 13, wherein the data structure is a directory entry for the file and the anti-virus state information is stored in a field in the directory entry.

17. The computer-readable medium of claim 13, wherein the data structure is an extra file fork for the file.

Rule ~~1.~~ 1.126

18 ~~19~~. The computer-readable medium of claim 17, further comprising: creating the extra file fork to hold the anti-virus state information.

19 ~~20~~. A computer system comprising:

a processor coupled to a system bus;

a memory coupled to the processor through the system bus;

a computer-readable medium coupled to the processor through the system bus;

a file system executed from the computer readable medium by the processor, wherein the file system causes the processor to store data structures associated with files on the computer-readable medium and further to retrieve the data structures from the computer-readable medium; and

an anti-virus process executed from the computer readable medium by the processor, wherein the anti-virus process causes the processor to store anti-virus state information for the file in the data structure associated with the file and further to obtain the anti-virus state information for the file from the data structure when the data structure has been retrieved.

20 ~~21~~. The computer system of claim 19 ~~20~~, wherein the anti-virus process further causes the processor to encrypt the anti-virus state information before storing it in the data structure and to decrypt the anti-virus state information when it is obtained from the data structure.

21 ~~22~~. The computer system of claim 19 ~~20~~, wherein the anti-virus process further causes the processor to compare the anti-virus state information stored in the data structure against corresponding information associated with a current version of the file to determine if virus scanning is required and to update the anti-virus state information if the anti-virus process causes the processor to scan the file as a result of the comparison.

22 ~~23.~~ The computer system of claim 19 ~~20~~, wherein the data structure containing the anti-virus state information is an entry in a file system directory and anti-virus process further causes the processor to store the anti-virus state information in the entry and to obtain the anti-virus state information from the entry.

23 ~~24.~~ The computer system of claim 19 ~~20~~, wherein the data structure containing the anti-virus state information is an extra file fork for the file and the anti-virus process further causes the processor to store the anti-virus state information in the extra file fork and to obtain the anti-virus state information from the extra file fork.

24 ~~25.~~ The computer system of claim 23 ~~24~~, wherein the anti-virus process further causes the processor to create the extra file fork to hold the anti-virus state information.

25 ~~26.~~ The computer system of claim 19 ~~20~~, wherein the data structure containing the anti-virus state information is stored as a resource in a resource fork for the file and the anti-virus process further causes the processor to store the anti-virus state information in the resource fork and to obtain the anti-virus state information from the resource fork.

26 ~~27.~~ A computer-readable medium having stored thereon a directory entry data structure for a file system comprising:

a file identifier field containing data representing a file system identifier for a file; and

a first reserved field containing data representing an anti-virus state for the file identified by the file identifier field.

27 ~~28.~~ The computer-readable medium of claim 26 ~~27~~, wherein the file comprises a data fork and a resource fork, the first reserved field contains data representing a two-byte checksum for the file and data representing two bytes of a three-byte length for the resource fork, and further comprising:

a second reserved field containing data representing a third byte for the resource fork length and data representing a three-byte length for the data fork.

28 ~~29.~~ A computer-readable medium having stored thereon a file fork data structure associated with a file comprising:

a file identifier field containing data representing a file system identifier for the file; and

a resource field containing data representing an anti-virus state of the file identified by the file identifier field.